

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-311134

(43)Date of publication of application : 07.11.2000

(51)Int.Cl.

G06F 15/00

G06F 13/00

G06F 19/00

(21)Application number : 11-120695

(71)Applicant : NIPPON YUNISHISU KK

(22)Date of filing : 27.04.1999

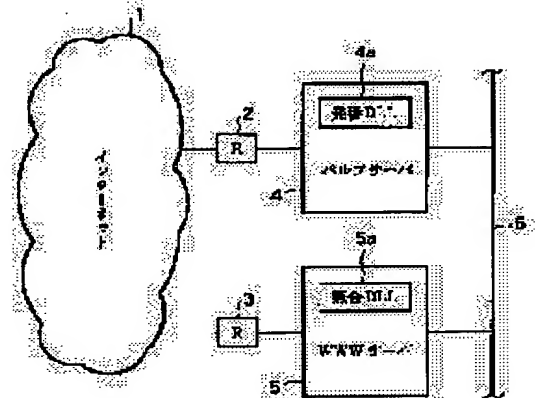
(72)Inventor : KASHIWAGI HIDEYUKI

(54) UNIT AND METHOD FOR ACCESS CONTROL AND SERVER SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent access congestion to a server by equipping a server system with a 1st server which issues an access number for specific access and a 2nd server which responds to a request having the access number.

SOLUTION: A 1st bubble server 4 and a 2nd WWW server 5 are interconnected through a network 6 and also connected to the Internet 1 through routers 2 and 3. Then the 1st bubble server 4 issues the number of access to the 2nd WWW server 5 by a numbering DLL as software for access from the Internet 1 and sends it out to a client. The client accesses the 2nd WWW server 5 by using the received access number, inquires whether the access number is effective using an inquiry DLL 5a, and sends information that the client requests to the client when the access number is effective.



LEGAL STATUS

[Date of request for examination] 27.04.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3378529

[Date of registration] 06.12.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Best Available Copy

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-311134

(P2000-311134A)

(43) 公開日 平成12年11月7日 (2000.11.7)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)
G 0 6 F 15/00	3 1 0	C 0 6 F 15/00	3 1 0 A 5 B 0 4 9
13/00	3 5 1	13/00	3 5 1 Z 5 B 0 8 5
19/00		15/26	5 B 0 8 9

審査請求 有 請求項の数19 O L (全 8 頁)

(21) 出願番号 特願平11-120695

(22) 出願日 平成11年4月27日 (1999.4.27)

(71) 出願人 591030237

日本ユニシス株式会社

東京都港区赤坂2丁目17番51号

(72) 発明者 柏木 秀幸

東京都港区赤坂二丁目17番51号 日本ユニ

シス株式会社内

(74) 代理人 100076428

弁理士 大塚 康樹 (外2名)

Fターム(参考) 5B049 BB49 CC06 EE51

5B085 AA08 AC03 AC16 BC07

5B089 GA11 GB03 HA10 JA21 JB22

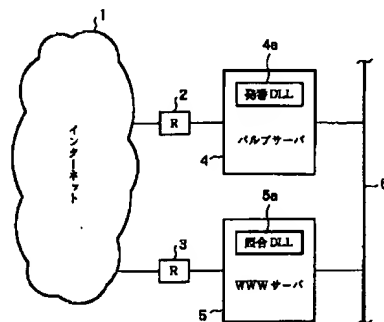
KA07 KC47 KC52 KH30 MA01

(54) 【発明の名称】 アクセス制御装置およびその方法、並びに、サーバシステム

(57) 【要約】

【課題】 コンサートチケットなどを予約するためのWWWサーバにおいては、アクセスが制限されていないため、アクセスの集中によるシステムダウンが引き起される可能性がある。

【解決手段】 バルブサーバ4は、インターネット1を介したアクセスに対して、アクセス番号を発行する。WWWサーバ5は、インターネット1を介したアクセスに対して、受信されるアクセス番号が有効か否かを判定し、有効なアクセス番号であれば、要求されるページを返す。



【特許請求の範囲】

【請求項1】 所定のアクセスに対してアクセス番号を発行する第一のサーバと、
前記アクセス番号を含む要求に対して応答する第二のサーバとを有することを特徴とするサーバシステム。

【請求項2】 さらに、前記アクセス番号を管理するデータベースを有することを特徴とする請求項1に記載されたサーバシステム。

【請求項3】 前記第一のサーバは、前記所定のアクセスがあると前記データベースからアクセス番号を取得し、取得したアクセス番号をそのアクセス元に送信することを特徴とする請求項2に記載されたサーバシステム。

【請求項4】 前記アクセス番号の発行可能数は動的に設定可能であることを特徴とする請求項1から請求項3の何れかに記載されたサーバシステム。

【請求項5】 前記第二のサーバは、要求に含まれるアクセス番号を前記データベースに照会し、有効なアクセス番号である場合に、要求される情報をその要求元へ送信することを特徴とする請求項2または請求項3に記載されたサーバシステム。

【請求項6】 前記アクセス番号の発行可能数は動的に設定可能であり、
前記第二のサーバは、要求に含まれるアクセス番号を前記データベースに照会し、有効なアクセス番号である場合に、要求される情報をその要求元へ送信することを特徴とする請求項1から請求項3の何れかに記載されたサーバシステム。

【請求項7】 さらに、前記アクセス番号の有効期間を管理するスケジューラを有することを特徴とする請求項1から請求項6の何れかに記載されたサーバシステム。

【請求項8】 前記所定のアクセスおよび前記要求はインターネットを介して行われることを特徴とする請求項1から請求項7の何れかに記載されたサーバシステム。

【請求項9】 所定のアクセスを受信する受信手段と、
前記アクセスに対してアクセス番号を発行する発行手段と、
前記アクセス番号を含む要求に対してサーバを制御する制御手段とを有することを特徴とするアクセス制御装置。

【請求項10】 さらに、前記アクセス番号を管理する管理手段を有することを特徴とする請求項9に記載されたアクセス制御装置。

【請求項11】 前記発行手段は、前記所定のアクセスがあると前記管理手段からアクセス番号を取得し、取得したアクセス番号をそのアクセス元に送信することを特徴とする請求項10に記載されたアクセス制御装置。

【請求項12】 前記アクセス番号の発行可能数は動的に設定可能であることを特徴とする請求項9から請求項11の何れかに記載されたサーバシステム。

【請求項13】 前記アクセス番号は暗号化されクッキーに登録されて送信されることを特徴とする請求項9から請求項12の何れかに記載されたアクセス制御装置。

【請求項14】 前記制御手段は、要求に含まれるアクセス番号を前記管理手段に照会し、有効なアクセス番号である場合に、要求される情報をその要求元へ送信するように前記サーバを制御することを特徴とする請求項10または請求項11に記載されたアクセス制御装置。

【請求項15】 前記アクセス番号の発行可能数は動的に設定可能であり、
前記制御手段は、要求に含まれるアクセス番号を前記管理手段に照会し、有効なアクセス番号である場合に、要求される情報をその要求元へ送信するように前記サーバを制御することを特徴とする請求項10または請求項11に記載されたアクセス制御装置。

【請求項16】 さらに、前記アクセス番号の有効期間を管理するスケジューラを有することを特徴とする請求項9から請求項15の何れかに記載されたアクセス制御装置。

【請求項17】 前記所定のアクセスおよび前記要求はインターネットを介して行われることを特徴とする請求項9から請求項16の何れかに記載されたアクセス制御装置。

【請求項18】 所定のアクセスを受信し、
前記アクセスに対してアクセス番号を発行し、
前記アクセス番号を含む要求に対してサーバを制御することを特徴とするアクセス制御方法。

【請求項19】 サーバの動作を制御するプログラムコードが記録された記録媒体であって、前記プログラムコードは少なくとも、
所定のアクセスを受信するステップのコードと、
前記アクセスに対してアクセス番号を発行するステップのコードと、
前記アクセス番号を含む要求に対してサーバを制御するステップのコードとを有することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はアクセス制御装置およびその方法、並びに、サーバシステムに関し、とくに、インターネット上のクライアントからアクセス要求を受け付けるアクセス制御装置およびその方法に関するものである。

【0002】

【従来の技術】http(Hyper Text Transfer Protocol)によりWebサイトを提供するWWW(World Wide Web)サーバは、アクセスを制限する方法をまったく備えないか、例えアクセスを制限するにしても、WWWサーバに加わる負荷を計測して、計測される負荷が所定値を超える場合にアクセスを制限する程度である。

【0003】また、WWWサーバに対する個々のアクセスは、アクセス数としてのみ捉えられている。

【0004】

【発明が解決しようとする課題】例えばコンサートチケットなどを予約するためのWWWサーバにおいては、アクセスが制限されていないため、アクセスの集中によるシステムダウンが引き起される可能性がある。

【0005】また、負荷が所定値を超える場合にアクセスを制限するWWWサーバの場合、WWWサーバに対するアクセスはアクセス数でしか把握されていないために、WWWサーバにアクセスして処理を行っているユーザは、その処理途中でアクセスが制限または不可にされる可能性がある。このような場合、WWWサーバにアクセスして一連の操作をしていたユーザは、WWWサーバにアクセスし直し、最初から操作をやり直さなければならない。

【0006】さらに、一つのWWWサーバに対して一台のクライアントマシンから同時に複数のアクセスを行うことが可能であるから、WWWサーバに対するアクセスがアクセス数でしか把握されていないと、一部のユーザによりWWWサーバのアクセスが独占されるような事態が発生する可能性もある。

【0007】本発明は、上述の問題を解決するためのものであり、サーバに対するアクセス集中を防ぐことを目的とする。また、サーバに対するアクセスをより詳しく把握し管理することを他の目的とする。

【0008】

【課題を解決するための手段】本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【0009】本発明にかかるサーバシステムは、所定のアクセスに対してアクセス番号を発行する第一のサーバと、前記アクセス番号を含む要求に対して応答する第二のサーバとを有することを特徴とする。

【0010】本発明にかかるアクセス制御装置は、所定のアクセスを受信する受信手段と、前記アクセスに対してアクセス番号を発行する発行手段と、前記アクセス番号を含む要求に対してサーバを制御する制御手段とを有することを特徴とする。

【0011】本発明にかかるアクセス制御方法は、所定のアクセスを受信し、前記アクセスに対してアクセス番号を発行し、前記アクセス番号を含む要求に対してサーバを制御することを特徴とする。

【0012】

【発明の実施の形態】〔構成〕図1は本発明にかかるアクセス制御装置を含むサーバ構成例を示す図である。

【0013】図1において、WWWサーバ5およびバブルサーバ4はLANなどのネットワーク6を介して相互に接続されているとともに、ルータ2および3を介してインターネット1へ接続されている。

【0014】バブルサーバ4は、インターネット1からWWWサーバ5へのアクセスを制御するアクセス制御装置とし

て機能する。詳細は後述するが、バブルサーバ4は、インターネット1からのアクセスに対してソフトウェアである発番DLL(Dynamic Link Library)によりWWWサーバ5へのアクセス番号を発行し、発行されたアクセス番号はクライアントへ送られる。

【0015】クライアントは、受信したアクセス番号を用いてWWWサーバ5にアクセスする。WWWサーバ5は、アクセスに利用されるアクセス番号が有効か否かを照合DLL5aにより照合し、有効なアクセス番号であれば、クライアントから要求される情報をクライアントへ送信する。

【0016】所定の期間、アクセス番号は有効であり、その期間、クライアントはWWWサーバ5からアクセスを拒否されることはない。このように、バブルサーバ4は、アクセス番号を発行する発行しないにより、WWWサーバ5へのアクセスを制御することができ、さらに、アクセス数だけでなく、アクセス番号によりクライアント(ユーザ)数を把握し、WWWサーバ5へのアクセスを制御することができる。

【0017】〔動作〕図2は図1に示すサーバ構成により実行されるアクセス制御を説明する図、図3および図4はアクセス制御の詳細、つまり発番DLL4aおよび照合DLL5aの処理を示すフローチャートである。

【0018】図3において、バブルサーバ4は、ステップS1でインターネットを介したアクセスを待ち、アクセスがあるとステップS2で、発番データベース(DB)7へアクセスして次のアクセス番号を取得する。なお、発番データベース7は、LAN6に接続されているデータベースサーバに配置するのが望ましいが、バブルサーバ4の中に配置することもできる。勿論、発番データベース7を通信回線を介して遠隔地に置くこともできる。

【0019】バブルサーバ4は、ステップS3でアクセス番号が取得できたか否かを判定し、取得できた場合はステップS4でアクセス番号を暗号化したキーにし、ステップS5でキーをクッキー(cookie)に登録し、クッキーおよびトップページをクライアント8へ送る。また、アクセス番号が取得できなかった場合はステップS6で「現在アクセス不可」を示すページをクライアント8へ送る。

【0020】バブルサーバ4からトップページを受信したクライアント8は、そのトップページにはWWWサーバ5のURL(Uniform Resource Locator)がリンクとして設定されている。クライアント8のユーザは、このリンクを選択することにより、WWWサーバ5にアクセスする。このアクセスの際、クッキーに登録されたキーがWWWサーバ5へ送られる。

【0021】図4において、WWWサーバ5は、ステップS11でインターネットを介したアクセスを待ち、アクセスがあるとステップS12で、受信されるキーを解読してアクセス番号(以下「受信アクセス番号」と呼ぶ)を得る。そして、ステップS13で受信アクセス番号を発番データベース7に照会し、ステップS14で受信アクセス番号が有

効か否かを判定する。受信アクセス番号が有効であればステップS15で、クライアント8から要求されるページをクライアント8へ送り、ステップS16で一連のページの操作が終了したなど、クライアント8によるページ操作が終了か否かを判定し、未了であればステップS11へ戻る。

【0022】従って、有効なアクセス番号をもつクライアント8から必要なページが要求されると、WWWサーバ5は、ステップS11からステップS15の処理を繰り返すことによって要求ページをクライアント8へ提供する。

【0023】一方、受信アクセス番号が無効の場合はステップS19で「アクセス番号が無効」を示すページをクライアント8へ送る。従って、WWWサーバ5は、有効なアクセス番号をもたないクライアント8からアクセスされたとしても「アクセス番号が無効」を示す以外のページを提供することはない。なお、「アクセス番号が無効」を示すページにはバブルサーバ4のURLをリンクとして設定しておくことが望ましい。

【0024】また、操作終了と判定した場合、WWWサーバ5は、ステップS17で受信アクセス番号の無効化を発番データベース7に指示し、ステップS18で終了ページをクライアントへ送信する。

【0025】このように、本実施形態によれば、アクセス制御をクライアント単位に行うことができる。言い換えれば、本来セッション管理ができないWWWサーバにおいて、クライアントを特定することでセッション管理を行うことが可能になる。

【0026】〔応用〕アクセス番号の無効化は、操作終了と判定された場合に限らず、発番データベース7側でスケジューラを稼働させ、定期的に古いアクセス番号を無効にする方法や、所定時間アクセスが途絶えた場合にアクセス番号を無効にする方法なども取り得る。

【0027】アクセスが集中し、大きな負荷が加わる可能性があるWebサイトに、本実施形態のアクセス制御を適用すれば効果的である。つまり、インターネット1を介したアクセスをバブルサーバ4により受け付け、予め設定されたアクセス（ユーザ）数だけアクセス番号を発行してWWWサーバ5へのアクセスを許可することができるので、例えば、バブルサーバ4へのアクセスが集中したとしても、アクセス番号を入手してWWWサーバ5へのアクセスを許可されたクライアント（ユーザ）は、アクセス集中の悪影響を受けることなく、WWWサーバ5に対する処理を続行することができる。従って、本実施形態のアクセス制御により、ユーザには快適な操作感を提供すること

が可能になる。

【0028】さらに、発番データベース7およびバブルサーバ4がWWWサーバ5から分離されているので、WWWサーバ5の並列化が容易である。勿論、発番データベース7をLAN6上などのデータベースサーバに配置すればバブルサーバ4の並列化も容易である。従って、サーバの並列化により負荷を分散して、Webサイトがさらに多くのアクセスに耐え得るようにすることもできる上、Webサイト全体を停止することなく動的にサーバを増設し、一部サーバを停止することができるので、Webサイトの増設やメンテナンスなどに好都合である。

【0029】また、アクセス番号は暗号化してクッキーに登録されるので、WWWサーバ5に対する不正なアクセスは困難であり、暗号化されたアクセス番号であるキーはクライアント8側に格納されるため、一台のクライアントマシンからWWWサーバ5に対して同時に複数のアクセスを行うことはできない。

【0030】さらに、アクセス番号の発行数は、発番データベース7を設定することで、任意に動的に変更することができるので、例えば、時間帯に応じてアクセス数を制御することができる。

【0031】本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を装置に供給し、その装置のCPUが記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成される。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現し、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0032】

【発明の効果】以上説明したように、本発明によれば、サーバに対するアクセス集中を防ぐことができる。また、サーバに対するアクセスをより詳しく把握し管理することで、サーバのユーザに対してより適切な処理を実行することができる。

【図面の簡単な説明】

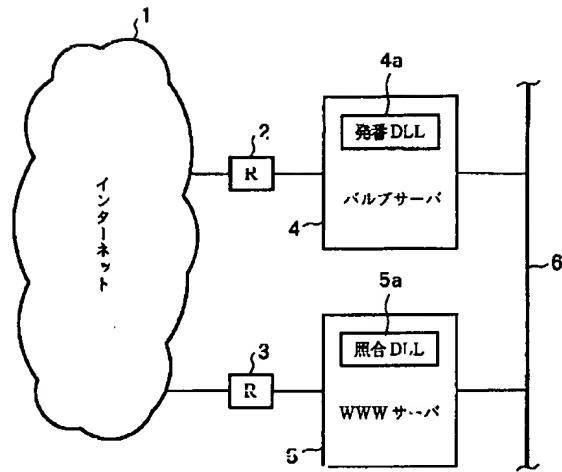
【図1】本発明にかかるアクセス制御装置を含むサーバ構成例を示す図、

【図2】図1に示すサーバ構成により実行されるアクセス制御を説明する図

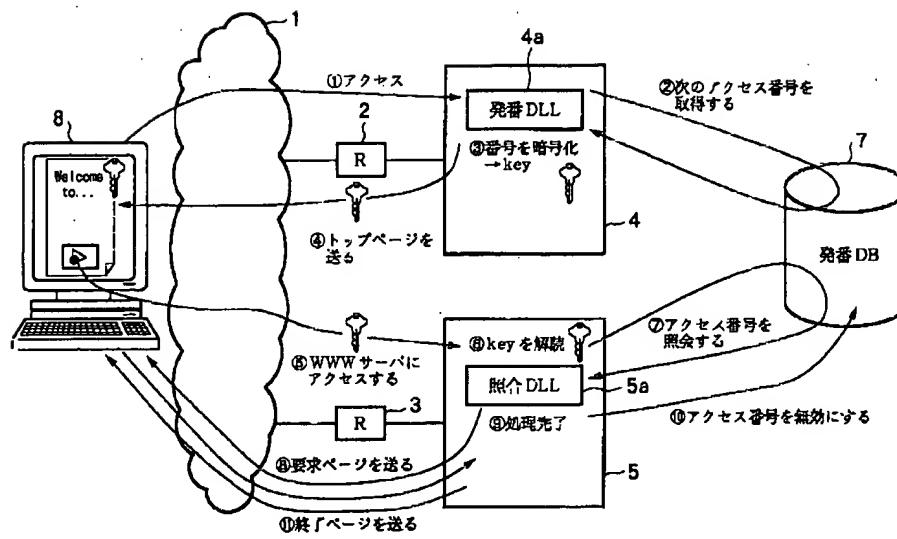
【図3】アクセス制御の詳細を示すフローチャート、

【図4】アクセス制御の詳細を示すフローチャートである。

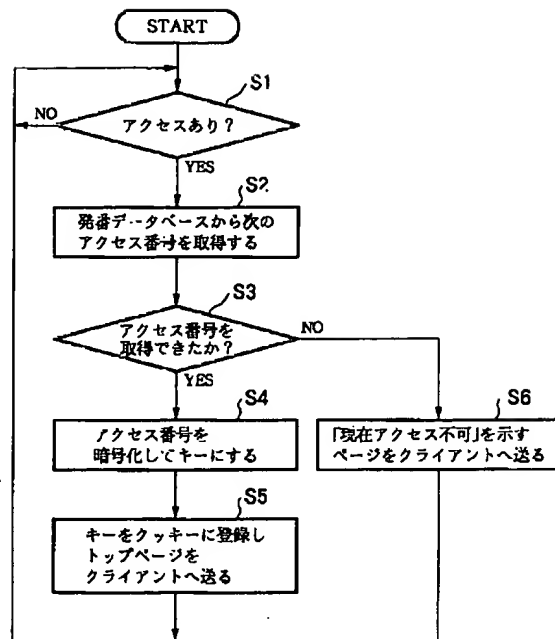
【図1】



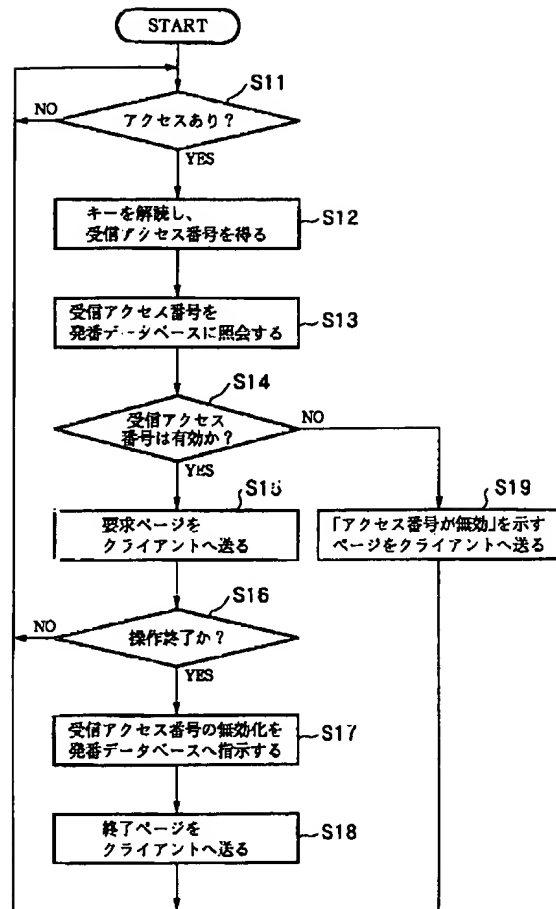
【図2】



【図3】



【図4】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.